

What is claimed is:

1. A system for providing consumer access to a financial account to implement a transaction comprising:

a biometric data capture device for reading consumer biometric data; and

a database server for generating a data storage key from the consumer biometric data received from the biometric data capture device and for retrieving a data record corresponding to the generated data storage key.

2. The system of claim 1 further comprising:

a payment device coupled to said biometric data capture device, said payment device generating a digital signature from said biometric data for a transaction message.

3. A system for supporting consumer access to a financial account by means of biometric data solely comprising:

a biometric data capture device for capturing biometric data corresponding to a consumer; and

a payment device for sending said captured biometric data to a merchant payment host as the identifier for the consumer's financial account data.

4. The system of claim 2 wherein said payment device generates a digital signature from said captured biometric data.

5. The system of claim 1 wherein the generated key is name data and the database server retrieves a plurality of data records corresponding to the generated key and determines whether biometric data stored in any of the retrieved data records corresponds to other biometric data received from a merchant purchase site.

6. A system for verifying access to a consumer's financial account comprising:

a database server for generating a data storage key from biometric data received from a transaction site; and

an identity database comprised of data records stored with reference to a data storage key corresponding to biometric data contained within the data record so that the database server may retrieve records from the identity database using data storage keys generated from the received biometric data.

7. The system of claim 6 wherein the database server generates a digital signature from biometric data retrieved from the identity database so that a transaction message may be verified.

8. A method for authorizing access to a financial account for a consumer comprising:

generating a data storage key from biometric data corresponding to a consumer; and

retrieving a data record corresponding to the generated data storage key, the data record containing financial account data for the consumer.

9. The method of claim 8 further comprising generating a digital signature from the biometric data corresponding to the consumer to authorize generation of electronic funds transfer messages for a financial transaction.

10. The method of claim 8 further comprising:

capturing the biometric data corresponding to the consumer; and

transmitting the captured biometric data so the data storage key may be generated.

11. The method of claim 9 further comprising comparing the generated digital signature to a received digital signature to authorize generation of electronic funds in response to said generated digital signature corresponding to said received digital signature.

12. The method of claim 8 wherein the generated key corresponds to name data and the retrieval includes:

retrieving a plurality of data records corresponding to the generated key; and

comparing the biometric data stored in the retrieved data records to other biometric data received from a merchant purchase site.

13. A method for accessing a financial account of a consumer comprising:

capturing biometric data corresponding to a consumer; and

sending the captured biometric data to a merchant payment host to obtain financial account data from the merchant payment host.

14. The method of claim 13 further comprising:

generating a digital signature from the captured biometric data; and

transmitting the generated signature in a transaction message to the merchant payment host for authorizing generation of electronic transfer messages by the merchant payment host.